Hans Journal of Wireless Communications 无线通信, 2016, 6(6), 117-122
Published Online December 2016 in Hans. http://www.hanspub.org/journal/hjwc
http://dx.doi.org/10.12677/hjwc.2016.66015

Hans汉斯

A Method of Disturbing Link Based on D-S Evidence Theory for Wireless Network

Xiaofeng Xu[1,2], Yongji Ren[3]

[1]Science and Technology on Communication Information Security Control Laboratory, Jiaxing Zhejiang
[2]No.36 Research Institute of CETC, Jiaxing Zhejiang
[3]Department of Command, Naval Aeronautical and Astronautical University, Yantai Shandong
Email: alickelly@126.com

Received: Nov. 25th, 2016; accepted: Dec. 8th, 2016; published: Dec. 15th, 2016

Abstract

The attack of signal link between nodes has a great destructive effect on the reliable operation and security of the wireless network. In this paper, a wireless link attack algorithm based on D-S evidence theory is proposed. Firstly, the method gives the formal definition of the link importance around the network nodes, and uses the basic reliability function to calculate the degree of importance. Then, according to the importance of Dempster combination rule, the importance of direct and indirect synthesis is obtained, and the importance of nodes in the process of link data transmission is obtained. On this basis, the attack is applied to the highest node important degree. Simulation results show that the algorithm can accurately attack the link between nodes, and achieve the effect of increasing the packet loss rate.

Keywords

Wireless Network, D-S Evidence Theory, Dempster Combination Rule, Link Disturbance

基于D-S证据理论的网络链路扰乱方法

许小丰[1,2]，任永吉[3]

[1]通信信息控制和安全技术重点实验室，浙江 嘉兴
[2]中国电科第三十六研究所，浙江 嘉兴
[3]海军航空工程学院指挥系，山东 烟台

文章引用: 许小丰, 任永吉. 基于 D-S 证据理论的网络链路扰乱方法[J]. 无线通信, 2016, 6(6): 117-122.
http://dx.doi.org/10.12677/hjwc.2016.66015

Email: alickelly@126.com

收稿日期：2016年11月25日；录用日期：2016年12月8日；发布日期：2016年12月15日

摘　要

节点间信号链路攻击对无线网络的可靠运行和安全保障具有极大的破坏作用。本文提出了一种基于D-S证据理论的无线链路攻击算法。该算法首先给出了网络节点周围链路重要性的形式化定义；利用基本信度函数计算直接重要程度，通过邻居节点的推荐获取间接重要程度；同时，根据Dempster组合规则对直接、间接重要性予以合成，从而得到链路数据传输过程中节点重要度排名。在此基础上，对重要度最高的节点进行攻击。仿真结果表明，本算法能够准确地攻击重要节点间链路，达到网络丢包率上升的效果。

关键词

无线网络，D-S证据理论，Dempster组合规则，链路扰乱

1. 前言

导致无线网络链路安全的原因还有：① 动态的拓扑结构；网络中的节点可能会经常性地改变它们的位置，因此网络的拓扑结构是高度动态的，这会导致一个节点的邻近节点频繁地发生变化，而这个节点又需要依赖邻近节点进行数据转发。② 无线通信；由于网络中的节点通过无线链路通信，任何装备了特定设备的入侵者都可以很容易地截获节点间的相互通信。③ 模糊的信任关系；实际的无线链路假设所有参与通信的节点都是诚实的，这就允许恶意节点通过发布错误的信息来使网络瘫痪[1]。

针对以上网络固有的特征，已有研究者提出很多针对链路的攻击方法。文献[2]中，研究人员对基于Petri网的随机网络攻击模型进行了分析，该模型对攻击组合中各组合部分之间的关联关系进行了详细的说明与论述，给出了攻击行为、攻击组合运算的定义和攻击组合的建立算法。同时，还对对该模型的组合结构及其复杂度进行了度量研究。该方法是针对网络中各种攻击方法提出的，通用性较强，但是没有有效区分网络节点及链路的重要性。文献[3]主要从网络中心战的角度对美Suter进化进行介绍。利用NCCT来收集并融合多个平台所获得的各类情报数据，然后无线远端注入信号，对对方网络的通信数据链进行阻断式干扰破坏。文献[4]使用层次扩展SPN对组合后的网络全局攻击行为进行建模。该方法通过对网络粗糙攻击路径的定义，从而挖掘出网络主机结点间潜在的攻击关系算法，可将这种方法直接用于对网络链路的干扰上去。文献[5]为了对网络攻击策略的有效性进行预期分析，该文提出了介数紧致系数、接近度紧致系数2个新的度量指标，并在考虑攻击代价条件下，理论分析了平均度、介数紧致系数、接近度紧致系数3个指标与攻击策略有效性的关系进行分析研究。文献[6]在仿真环境下对网络攻击与干扰的方法与效果进行分析研究。该文将遗传算法运用到网络攻击实践中，根据网络全局与局部的不同特性，对节点攻击图谱进行优化，提高攻击的指向性。文献[7]综述了当前常用的安全防御与网络攻击方法，对利用病毒、木马、拒绝服务等攻击方法进行了简单的介绍，并对基于网络的路由、链路等的安全策略的准则进行相关分析与描述。

以上方法都没有考虑到实际无线网络中节点间的层次关系，即网络中节点重要性不同；根据节点间链路重要性不同，节点转发数据的负载也是不同的。因此，对不同的节点进行攻击的效果也是不同的。

针对上述研究工作中存在的不足，本文提出了一种基于 D-S 证据理论的信号链路攻击方法。给出了网络节点链路重要性的形式化定义；根据 Dempster 组合规则得到数据传输过程中节点重要度排名，在此基础上，对重要度最高的节点链路进行假冒攻击。

2. 相关定义及规则

D-S证据理论[8] [9]基于由互斥且穷举的基本命题所构成的集合Ω，称为识别框架。2^{Ω}是Ω的幂集，是基于Ω的所有可能命题的集合。这里将Ω定义为$\{T,-T\}$，T和$-T$代表节点两种互斥且穷举的信任状态，即可信和不可信。2^{Ω}为$\{\Phi,\{T\},\{-T\},\{T,-T\}\}$，其中的$\{T\}$，$\{-T\}$和$\{T,-T\}$分别表示“节点高重要性”，“节点不重要性”和“节点一般重要性”的命题。

本文中节点重要性值定义[10]为向量形式：$\left(m(\{T\}),m(\{-T\}),m(\{T,-T\})\right)$，其中：$m(\{T\})$表示信任证据对节点性高重要性的支持程度，$m(\{-T\})$表示信任证据对节点不重要性的支持程度，$m(\{T,-T\})$表示了信任证据的一般重要性的支持程度。$\mathrm{Bel}(T)=m(\{T\})$，$\mathrm{Pl}(T)=m(\{T\})+m(\{T,-T\})$，中性区间宽度为$m(\{T,-T\})$。

本文中节点重要性的合成实际上是多个证据的组合，遵循 Dempster 组合规则：

$$\begin{cases} m(A)=m_1(A)\oplus m_2(A) \\ \qquad =\dfrac{\sum\limits_{X\cap Y=A} m_1(X)\times m_2(Y)}{1-K} \\ \qquad A\neq\varnothing,\ A\subseteq\Omega \\ m(\varnothing)=0 \end{cases}$$

$$K=\sum_{X\cap Y=\varnothing} m_1(X)\times m_2(Y)$$

3. 节点重要性评估模型

在无线网络中，当需要评估节点的重要性时，需要考虑两方面的因素。一方面是节点对其邻居链路数据的成功转发率，记为直接重要程度$\boldsymbol{D}$；另一方面是节点对非邻居链路数据的成功转发率，记为间接重要程度$\boldsymbol{I}$。

3.1. 直接重要程度

在无线网络中，依据直接数据交互历史来计算节点的直接重要程度。首先定义了一个识别框架$\theta=\{T,\sim T\}$，T 表示成功转发，$\sim T$ 表示拒绝转发。节点的直接重要程度定义为一个向量 $\boldsymbol{D}$，$\boldsymbol{D}=\left(m(\{T\}),m(\{\sim T\}),m(\{T,\sim T\})\right)$，其中 $m(\{T\}),m(\{\sim T\}),m(\{T,\sim T\})$ 分别表示链路成功转发包的比率，明显拒绝转发包的比率以及对于是否成功转发包不确定的比率，它们的值分别用 α,β,γ 来表示，并且满足 $0\le\alpha,\beta,\gamma\le1,\alpha+\beta+\gamma=1$。

由于节点重要程度的动态性，需要在时域上来研究节点间链路的重要程度。初始时刻，节点 i 和邻居节点 j 之间由于没有交互历史，因此节点 i 相对节点 j 的直接重要程度 $\boldsymbol{D}_{i,j}(t_0)=(0,0,1)$，节点更新其 $\boldsymbol{D}$ 的时间周期为 Δt (常量)。当 $t=t_n$ 时，$\boldsymbol{D}_{i,j}(t_n)=(\alpha_n,\beta_n,\gamma_n)$，$\Delta t$ 以后，即 $t=t_{n+1}=t_n+\Delta t,\ D_{i,j}(t_{n+1})=(\alpha_{n+1},\beta_{n+1},\gamma_{n+1})$。按照如下方式更新节点 i 的直接重要程度：$\boldsymbol{D}'_{i,j}(t_{n+1})=(1-w)*D_{i,j}(t_n)+w*D_{i,j}(t_{n+1})=(\alpha'_{n+1},\beta'_{n+1},\gamma'_{n+1})$，其中 w 是一个常量，表示权重系数。在直接重要程度的更新过程中，节点 i 将动态选择 w 的值，如果$(\alpha_{n+1}-\alpha_n)\ge(\beta_{n+1}-\beta_n)$，那么 $w=w_1$；否则，即$(\alpha_{n+1}-\alpha_n)<(\beta_{n+1}-\beta_n)$，那么 $w=w_2$，其中 w_1、w_2 满足：$0\le w_1\le0.5\le w_2\le1$。动态选择 w 能够同时

关注当前时刻和前一时刻的直接重要程度，而且 $w_1 \angle w_2$ 体现了当前时刻对直接重要程度的影响大于前一时刻。

通过上述步骤，可以有效的更新节点的直接重要程度，对网络的动态变化做出实时的响应。为了表述方便，下文中的 $\boldsymbol{D}_{i,j}(t_n)$ 简写成 $\boldsymbol{D}_{i,j}$。

3.2. 间接重要程度

在无线网络中，除了需要考虑节点 i 相对邻居节点的重要程度，还要考虑相对非邻居节点 j 的重要程度，即对非邻居节点间链路数据的成功转发率。

攻击方从网络外部获取节点 i 对非邻居节点数据的成功转发率时，往往由于观测值的不全面而导致节点间接重要程度与直觉相悖，产生不合理的结果。本文采用 C. K. Murphy 等人提出的折扣系数 $\text{factor}=[f_1,\cdots,f_k]$ 解决该问题。

节点 i 相对节点 j 的间接链路重要程度记作 $I_{i,j}$。假定分别得到了 k 个不同的节点 i 相对节点 j 的间接重要程度向量 $I_{n_1,j}=\left(m_{1,j}(\{T\}),m_{1,j}(\{\sim T\}),m_{1,j}(\{T,\sim T\})\right),\cdots,I_{n_k,j}=\left(m_{k,j}(\{T\}),m_{k,j}(\{\sim T\}),m_{k,j}(\{T,\sim T\})\right)$，通过证据的距离公式，可以计算出这 k 个间接重要程度向量中任意两个向量 p,q 之间的证据距离 $d_{p,q}$，它反映了第 p_{th} 个间接重要程度与第 q_{th} 个间接重要程度之间的冲突程度。 p,q 的相似度记作 $s_{p,q}$，那么 $s_{p,q}=1-d_{p,q}$，$s_{p,q}=s_{q,p}$。这样，所有的 $s_{p,q}$ 构建了一个下式所示的 $k*k$ 的间接重要程度向量的相似度矩阵 S。

$$S=\begin{vmatrix} 1 & s_{1,2} & \cdots & s_{1,k} \\ s_{2,1} & 1 & \cdots & s_{2,k} \\ \vdots & \vdots & \vdots & \vdots \\ s_{k,1} & s_{k,2} & \cdots & 1 \end{vmatrix}_{k*k}$$

由 D-S 证据理论可以得知，当证据发生冲突的时候，如果一个证据与其他大多数证据保持一定程度的一致性，则认为这个证据应该对最终的融合结果产生较大的影响，相反，如果一个证据与其他大多数证据都不一致，那么应该减小这个证据对最终的融合结果的影响。因此，每个证据的权重与被其他证据的综合支持程度成正比；那么在获得了证据的相似度矩阵后，通过矩阵分析的方法来决定每个推荐信任向量的权重。

假定对第 p_{th} 个间接重要程度向量的支持度为 η_p，那么 $\eta_p=\sum_{q=1,\ q\neq p}^{k} S_{p,q}$，其标准权重 $\chi_p=\eta_p\Big/\sum_{q=1}^{k}\eta_q$，并且满足 $\sum_{p=1}^{k}\chi_p=1$。选择标准权重系数中最大的系数 $\chi_{\max}$ 作为关键证据，然后就可以得到每个向量的折扣系数 $\text{factor}=[f_1,\cdots,f_k]=[\chi_1,\cdots,\chi_k]/\chi_{\max}$，最后根据折扣因子 factor 对节点 i 的间接重要程度向量做如下修正：

$$\begin{cases} m_i'(A)=f_i*m_i(A), A\subset\theta \\ m_i'(\theta)=1-f_i+f_i*m_i(\theta)=1-\sum m_i'(A) \end{cases}$$

这样，就可以得到修正后间接重要程度 $I_{i,j}'$。由上述方法可知，与其他向量的冲突越严重，其折扣系数就越小，对间接重要程度的最终合成的影响就越弱。

3.3. 综合重要程度

在得到相对节点 j 的通信链路修正后的直接重要程度 $D_{i,j}'$ 和间接重要程度 $I_{i,j}'$，根据 Dempster 组合规则对 $D_{i,j}'$ 和 $I_{i,j}'$ 进行合成以得到对节点 i 相对节点 j 的综合链路重要程度 $S_{i,j}$，

$S_{i,j}=\left(m_{i,j}^{*}\left(\{T\}\right),m_{i,j}^{*}\left(\{\sim T\}\right),m_{i,j}^{*}\left(\{T,\sim T\}\right)\right)$，其满足下述条件：

$$\begin{cases} m_{i,j}^{*}(A)=\left(\left(m'_{n_1,j}(A)\oplus m'_{n_2,j}(A)\right)\oplus\cdots\right)\oplus m'_{n_k,j}(A)\oplus m_{i,j}(A),\ A\subset\theta \\ m_{i,j}^{*}(\varphi)=0 \end{cases}$$

因此，节点 i 的综合重要程度 $S_i=\sum_{j=1\cdots n}^{j\neq i}S_{i,j}$，这里 n 为网络中节点数量。根据节点重要性排名，在敌对网络中选择重要性最高的节点进行扰乱，从对整个无线网络的数据传输及连通性造成最大的破坏效果。

4. 实验分析

实验场景设置如下：20个节点随机布撒在100 m × 100 m检测区域；节点通信半径为20 m；根据实验攻击过程设置恶意攻击节点；通过采用选择性重发攻击方法进行仿真验证。

如仿真实验图(图1)所示，当只对一般节点链路进行恶意攻击时，网络整体丢包率缓慢增加；网络最高丢包率只要30%左右，最低丢包率达到20%；这是因为发起的攻击全部都是针对不重要的节点实施的。当进行随机攻击时，网络整体丢包率基本保持稳定，最高丢包率达到40%左右，最低丢包率达到30%左右；这是因为随机攻击过程中既有一般节点，也有重要节点，因此丢包率比较平均。当对重要节点进行攻击时，网络整体丢包率迅速增加；这是因为攻击重要节点，对网络的性能影响最大，可以使整个网络瘫痪。由此可见，利用本文所提出的方法对网络中重要链路进行选择重传攻击，可以对无线网络通信性能起到更大的破坏作用。

5. 结论

链路攻击对无线网络的可靠运行和安全保障具有极大的破坏作用。本文提出了一种基于D-S证据理论的信号链路攻击新方法。主要工作有：1) 利用证据理论实现了节点链路重要性的定义和量化；2) 分别制定节点链路直接、间接重要度，并利用Dempster组合规则对直接、间接重要性予以合成；3) 对过程中综合链路重要度最高的节点进行选择重发攻击实验验证；实验结果表明；本文算法能实时、准确地攻击网络重要节点及其链路，达到对方网络丢包率大量增加的效果。

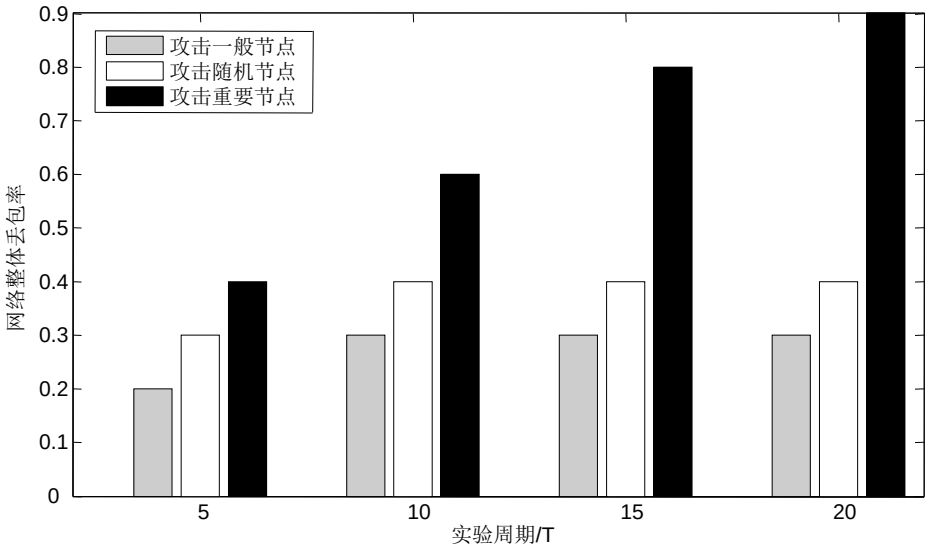

Figure 1. Simulation experiment for network packet loss rate
图 1. 网络丢包率

基金项目

国家自然科学基金资助项目(61070170)。

参考文献 (References)

[1] 杜欣军. Ad Hoc 网络安全问题的研究[D]: [博士学位论文]. 西安: 西安电子科技大学, 2004.

[2] 高翔, 祝跃飞, 刘胜利. 一种基于广义随机着色 Petri 网的网络攻击组合模型[J]. 电子与信息学报, 2013, 35(11): 2608-2614.

[3] 赵敏. 网络中心战的网络攻击——Suter 计划[J]. 现代防御技术, 2012, 39(6): 139-143.

[4] 黄光球, 张斌. 基于层次扩展 SPN 的网络攻击模型[J]. 计算机工程, 2012, 37(22): 12-23.

[5] 覃俊, 吴泓润. 代价下复杂网络攻击策略有效性研究[J]. 北京理工大学学报, 2013, 33(1): 5-10.

[6] 牛雪婷. 网络攻击节点图谱最优化过程的仿真分析[J]. 科技通报, 2013, 29(12): 121-123.

[7] 杨乐. 网络攻击与防御策略分析研究[J]. 数字技术与应用, 2014(1): 172-173.

[8] Dempster, A. (1967) Upper and Lower Probabilities Induced by Multivalued Mapping. *Annals of Mathematical Statistics*, **38**, 325-339. https://doi.org/10.1214/aoms/1177698950

[9] Shafer, G. (1976) A Mathematical Theory of Evidence. Princeton University Press, Princeton, NJ.

[10] 成坚, 冯仁剑, 许小丰, 万江文. 基于 D-S 证据理论的无线传感器网络信任评估模型[J]. 传感技术学报, 2009, 22(12): 1802-1807.